UNITED STATES DISTRICT COURT

DISTRICT OF MONTANA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Michael Robinson, being duly sworn, hereby state as follows:

BACKGROUND OF AFFIANT

1. I, Michael Robinson, am currently a Detective with the Billings Police Department assigned to the Eastern Montana High Intensity Drug Task Area (EMHIDTA) Task Force and a Task Force Officer for the United States Postal Inspection Service. This appointment started in April 2024. Prior to the assignment with the USPIS to EMHIDTA, I became a Police Officer with the Billings Police Department in March of 2003. I have worked approximately eight years as a uniformed patrol officer. I have also worked approximately thirteen years as a Detective for the Billings Police Department. For five of those thirteen years I was assigned to the general investigations division. In this division, I investigated all types of crimes to include crimes against children, financial crimes, homicides and more. For the other eight years as a Detective, I was assigned to EMHIDTA and worked drug crimes. Seven of those eight years I was assigned to the Federal Bureau of Investigations as a TFO. I have been assigned to work federal, state, and local narcotics investigations but target federal interstate narcotics investigations.

2. As a Postal Inspector Task Force Officer, I investigate to prevent the flow of illicit drugs and contraband through the United States Mail. I have assisted with investigations involving the distribution of controlled

substances. I have also participated in narcotics investigations which have resulted in the seizure of large quantities of controlled substances such as cocaine, marijuana, methamphetamine, fentanyl, and heroin. I am familiar with and have participated in all of the normal methods of investigation, including but not limited to visual surveillance, questioning of witnesses, the use of search and arrest warrants, the use of informants, and the use of the Grand Jury. Additionally, I have consulted with other agents who have been involved in similar investigations.

3. This affidavit is based upon information I have gained through training and experience, as well as upon information provided to me by other individuals, including law enforcement officers.

4. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known concerning this investigation but have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence relating to violations of 21 U.S.C. § 841(a)(1) and 21 U.S.C. § 846, are located in a black Samsung T-Mobile cell phone with IMEI (International Mobile Equipment Identity) Number 354519744960239 (hereafter referred to as Device). The Device is currently located at the EMHIDTA Office (evidence vault) located in Billings, MT. (see Attachment A).

5. I am familiar with the facts and circumstances of this investigation, as set forth in this affidavit, as a result of the following: (1) my training and experience; (2) my personal involvement in this investigation; (3) my discussions with other federal, state, and local law enforcement familiar

with this investigation; (4) my review of reports and other documents prepared by federal and local law enforcement officers; (5) physical surveillance conducted by federal agents or local law enforcement agencies, which has been reported to me either directly or indirectly.

PURPOSE OF AFFIDAVIT

6. This affidavit is made in support of a search warrant for evidence, fruits, and instrumentalities of conspiracy to possess with intent to distribute controlled substances, possession with intent to distribute, and distribution of controlled substances, in violation of 21 U.S.C §§ 841(a)(1) and 846, as those items are set forth in Attachment B, at the following location, which is further described in Attachment A. The item to be searched is described as a black Samsung T-Mobile cell phone with IMEI (International Mobile Equipment Identity) Number 354519744960239 (hereafter referred to as Device). The Device is currently located at the EMHIDTA Office (evidence vault) located in Billings, MT. (see Attachment A).

7. The applied for search warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

8. Based on my training and experience, I use the following terms to convey the following meanings

a. **Wireless telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. **Data:** means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

c. **Email** or **electronic mail:** means messages transmitted over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, computer networks, and minicomputers have an email system. Sent messages are stored in electronic mailboxes at least until the recipient retrieves them. After reading electronic mail, recipients can store it on their computer as a file, forward it to other users, or delete it, or they may store the

message on a remote server, such as the one from which they may have retrieved the email.

d. **Image** or **copy:** refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

e. ***Internet:*** *is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.*

f. **Text Messages:** are a form of communication through the use of cellular telephones or handheld electronic devices upon an electronic service provider's network or system. A message normally contains text composed by the sender, usually input via a lettering system on the device or computers keypad. The message can also be an image or short video sent or received.

g. **Uniform Resource Locator:** (URL) *are typically used to access web sites or other services on remote devices such as http://www.usdoj.gov, for example.*

h. **Voice Mail:** means a computerized system for answering incoming phone calls and allowing the caller to leave a message, which may be later retrieved.

i. **World Wide Web:** can be considered a massive database of information that is stored on linked computers that make up the Internet. This information can be displayed on a computer in the form of a web page, which is a document on the World Wide Web. A web site is a related collection of files and can consist of any number of web pages.

OVERVIEW AND INTRODUCTION OF BACKGROUND INVESTIGATION

9. Based on my training, experience, and research, I know that smartphone devices, such as the Device, have capabilities that allow them to serve as a wireless telephone, data storage device, and digital camera and that smartphone devices can connect to the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, who the user was communicating with, and the content of those communications. I also know the devices would allow to store text messages and digital images of, or related to, the possession or distribution of controlled substances or firearms.

10. Based upon my knowledge, training and experience in investigating federal narcotics crimes, and the experience and training of other law enforcement officers with whom I have had discussions, I am aware of the following:

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION AND FORENSIC ANALYSIS

11. It is not possible to determine, merely by knowing the cellular telephone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data

stored on the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "airplane mode" which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

12. Following the issuance of this warrant, the Device will be subjected to a forensic analysis. All forensic analyses of the data contained within the telephone and its memory cards will employ search protocols

directed exclusively to the identification and extraction of data within the scope of this warrant and will follow the procedures below.

13. Based on my knowledge, training, and experience, I knows that electronic devices, such as smartphones, can store information for long periods of time. Similarly, items that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

14. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how

electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. The affiant knows that when an individual uses an electronic device to facilitate drug trafficking, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of facilitating the criminal offense, for example, communicating with sources or customers. The electronic device is also likely to be a storage medium for evidence of crime. From his training and experience, the affiant believes that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

15. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant the affiant is applying for would permit an agent's seizure and subsequent review of the Device as well as the forensic examination

of the Device consistent with the warrant. The examination will require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

16. Following the issuance of this warrant, an agent will seize the Device and submit the Device for a forensic extraction of the Device. Subsequently, the forensic extraction will be examined for evidence described in Attachment B. All searches and forensic analysis of the data contained within the Device and its memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant. If evidence relating to another crime is discovered, agents will not look for additional evidence relating to the new crime without first applying for and obtaining a search warrant for that new crime.

17. Based on the foregoing, identifying, and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days, absent further application to this court.

18. In searching digital data stored on digital devices, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel will complete the search as soon as is practicable but not to exceed 120 days from the date of execution of this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 120-day period from the date of execution of the warrant.

b. The team searching the digital devices will do so only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

    i. The team may subject all of the data contained in the digital device or the forensic copy capable of containing items to be seized as specified in this warrant to the protocols to determine whether the digital device and any data falls within the items to be seized as set forth herein. The team searching the digital device may also search for and attempt to recover "deleted," "hidden" or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized as set forth herein.

    ii. These search protocols also may include the use of tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the team searching the digital device shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the team searching a digital device pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending

further order of Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. At the conclusion of the search of the digital devices, any digital device determined to be itself an instrumentality of the offense(s) and all the data thereon shall be retained by the government until further order of court or one year after the conclusion of the criminal case/investigation.

f. Notwithstanding, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized in this warrant on any retained digital devices or digital data absent further order of court.

g. If the search team determines that a digital device is not an instrumentality of any offense under investigation and does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will as soon as practicable return the digital device and delete or destroy all the forensic copies thereof.

h. If the search determines that the digital device or the forensic copy is not an instrumentality of the offense but does contain data falling within the list of the items to be seized pursuant to this warrant, the government either (i) within the time period authorized by the Court for completing the search, return to the Court for an order authorizing retention of the digital device and forensic copy; or (ii) retain only a copy of the data found to fall within the list of the items to be seized pursuant to this warrant and return the digital device and delete or destroy all the forensic copies thereof.

PROBABLE CAUSE

19. On 5/20/24, United States Postal Inspector Mike Smith obtained a federal search warrant for a United States Postal Service Priority Mail parcel going to Reyna P. Ardorin at 2757 1st St W in Worden, MT 59088. The sender of the parcel was Edward Werner Federal Defenders of Montana, Billings MT. The parcel had a tracking number of 9505515465974135782825.

20. On 5/20/24, the parcel was searched and inside Agents located four separate bags containing suspected narcotics. The bags were concealed in other items. One bag contained a white crystalline substance that weighed approximately 449.85 grams. A sample of this was tested using a presumptive test kit and was positive for methamphetamine. Three other bags were found that contained a white powder substance that weighed approximately 303.35 grams. A sample from one of the three bags was tested using a presumptive test kit and was positive for cocaine. All the narcotics were removed from the parcel for the safety of the community. The other miscellaneous items were placed back into the parcel and sealed.

21. On 5/22/24, an individual called the Worden Post Office and inquired about the delivery status of this parcel. The individual provided a name of Reynard Dublunch and a phone number of 415-214-4035. Agents later learned that "Reynard Dublunch" was actually Reynard Porche.

Dublunch is Porche's middle name and it appeared he used it as his last name in an attempt to conceal his true identity.

22. I researched the phone number using a nationwide database search and it returned to a Reynard Dublunch Porche with a Date of Birth of XX/XX/1972. I ran a criminal history check on Porche and found that he had arrests for gun violations in 1997, 2021 and 2022, possession of controlled substances with intent to distribute in 2015 and 2021, sex with minor in 2008, and several driving under the influence arrests, as well as other arrests.

23. On 5/23/24, the same individual called again and stated they would come to the Post Office later in the afternoon to pick up the parcel. Agents got in the area of the Worden Post Office and waited for someone to pick the parcel up. A male entered the Post Office and requested the parcel. It was turned over to him and he exited the Post Office with the parcel. He was detained outside by Agents and identified as Reynard Porche. Porche had in his possession his truck keys, a cell phone (Device) and wallet.

24. USPI Smith and I conducted a mirandized recorded interview with Porche. He agreed to talk to Agents and provided the following information: Porche provided his cell phone number as 415-214-4035 and the Device was his only cell phone he had. Porche stated he got a text message from an unknown phone number and person last week stating that he would be getting a package sent to him. They provided him a tracking number for the package. He later changed this statement

and claimed he got a phone call and not a text message. Porche stated he was unsure who the caller was. Porche also claimed he spoke to a female at the Federal Defenders Office in Billings a few days after receiving the call from the unknown individual and expected property seized in a previous case was to be returned to him. He claimed this was what he believed was in the package. Porche denied knowing about any drugs being in the parcel. Porche then claimed he was being set up by either the federal government or the "mafia." Agents asked more questions about the mafia and all Porche would say is that it involved the Mexican Cartel. Porche then admitted to being a meth user and admitted he recently used meth. Agents asked for consent to search his truck for evidence, and he provided consent. A digital scale was found in his center console. I know that a digital scale is commonly used by drug distributors to weigh out drugs prior to distributing them.

25. Agents told Porche they wanted to confirm his story about getting a phone call from someone last week and asked for consent to search the Device. Porche declined to give consent for the Device. Using USP data available to us, Postal Inspector Smith and I were aware that someone had remotely checked the tracking information regarding the package frequently prior to the attempted pick up by Porche. We asked Porche about this, and Porche admitted to using an app on the Device to check the status of the parcel.

26. After the interview was concluded, Porche was arrested and transported to the Yellowstone County Detention Center and a federal hold was

placed on him. I maintained possession of the Device until it was placed in the evidence vault at EMHIDTA.

CONCLUSION

27. In this matter I submit there is probable cause to believe that evidence, fruits, and instrumentalities of conspiracy to possess with intent to distribute controlled substances, possession with intent to distribute, and attempted possession of controlled substances with intent to distribute, in violation of 21 U.S.C §§ 841(a)(1) and 846, as those items are set forth in ATTACHMENT B, will be located inside the Device. The Device is currently located at the EMHDITA Office (evidence vault) located in Billings, MT.

Michael Robinson
Postal Inspector Task Force Officer
United States Postal Inspector Service

Subscribed and sworn to before me on the 29 day of May, 2024.

Honorable Timothy J. Cavan
United States Magistrate Judge
District of Montana